

REMARKS

In view of both the amendments presented above and the following discussion, the Applicants submit that none of the claims now pending in the application is obvious under the provisions of 35 USC § 103. Thus, the Applicants believe that all of these claims are now in allowable form.

If, however, the Examiner believes that there are any unresolved issues requiring adverse final action in any of the claims now pending in the application, the Examiner should telephone Mr. Peter L. Michaelson, Esq. at (732) 542-7800 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Interview Summary

The Applicants' representative conducted a telephonic interview with the Examiner commencing at approximately 2 PM on April 19, 2006. This interview addressed the pending § 103 rejection in this application and specifically the Applicants sought clarification from the Examiner as to the basis of the rejection and her interpretation of the claim 15 as it then stood. The Applicants also presented their view of the rejection and claim 15. No specific claim amendments were discussed.

For brevity, the Examiner's views are discussed in the next section of this amendment which addresses the obviousness rejection of claim 15.

Appl. No. 10/019,344
Amdt. dated June 26, 2006
Reply to final Office action of Jan. 26, 2006

The Applicants sincerely thank the Examiner for the opportunity to have conducted the interview and for all the courtesies she extended to the Applicants' representative in connection therewith.

Specification amendments

Various amendments have been made to the specification to correct minor inadvertent typographical errors that remained in the specification.

Status of claims

Claim 15 has been amended. No other claims have been amended. No claims have been cancelled or added.

Rejections under 35 USC § 103

1. Claims 15, 16, 17 and 24

The Examiner rejected independent claim 15 and dependent claims 16, 17 and 24, under the provisions of 35 USC § 103, as being obvious over the teachings in the Moroney et al patent (United States patent 5,054,067 issued to P. Moroney et al on October 1, 1991) in view of the Kocher et al patent (United States patent 6,327,661 issued to P. C. Kocher et al on December 4, 2001). In view of the amendment now made to claim 15, this rejection is respectfully traversed.

Specifically, the Examiner take the position that the Moroney et al patent substantially teaches loading

plaintext and an encryption key into a shift register, that has both linear and non-linear feedback functions, to produce a pseudorandom non-linear sequence. However, the Examiner concedes that this patent fails to teach use of this method as it would apply to protecting a smart card from attack. Given that failing, the Examiner then turns to the Kocher et al patent for its teachings of a method to clock a microprocessor in a smart card wherein a pseudo-random number generator is used to implement clock-skipping and thus protect the card from attack. Specifically, col. 6, line 65 through col. 7, line 18 of that patent, teaches that the clock interval is intentionally randomly varied to increase the difficulty of detecting cryptographic operations through detection of the card's power consumption and/or electromagnetic radiation produced by the card. Given these teachings, the Examiner concluded that it would have been obvious for one skilled in the art to simply incorporate a shift register containing both linear and non-linear feedback elements, as taught by the Moroney et al patent, into the arrangement taught by the Kocher et al patent as a way to generate pseudo-random timing patterns that would defeat cryptanalysis to a greater extent than that provided through the teachings of the Kocher et al patent alone, and, by doing so, arrive at the Applicants' present invention.

As the Examiner will shortly appreciate, her conclusion is not correct with respect to claim 15, as it currently stands.

For the sake of brevity, the Applicants will not summarize the salient teachings of the Moroney et al and

Kocher et al patents, but instead will simply direct the Examiner's attention to the Applicants' prior amendment mailed November 4, 2006, and particularly the second full paragraph on page 12 through the partial full paragraph on the top of page 15, for that summarization.

As set forth in that amendment, the Applicants have recognized that by appropriately and independently controlling both the linear and non-linear feedback functions in their inventive shift-register based apparatus, the leakage data can be made sufficiently resistant to statistical analysis. While doing so is advantageously relatively simple and economical to implement, a significant degree of additional protection against cryptanalysis results.

The Applicants have now amended claim 15 to recite that the linear and non-linear feedback elements "function separately from each other", i.e., are independent of each other.

If, as the Examiner postulates, the teachings of the Moroney et al patent, particularly regarding the use of linear and non-linear shift register feedback elements, were to be incorporated into the arrangement taught by the Kocher patent and presumably (given that the Examiner does not specify exactly where) into clock skipping module 240, then the linear and non-linear feedback elements would function together and not independently of each other. Why?

Examination of the Kocher et al patent, specifically FIG. 2 which shows the clock-skipping module as

part of the overall clocking circuitry, indicates a single clock line 220 applied to the clock skipping module and a single clock line 260 applied to both microprocessor core 225 and cryptographic accelerator 280. In that regard, this patent expressly states in col. 7, line 20 et seq and in pertinent part:

"Referring now to FIG. 2, random number generator 200 ... is used to determine which clock cycles (or clock state transitions) are to be used by microprocessor core 225. ... Clock skipping module 240 then combines ... random output 205 with clock signal 220 received from external smartcard interface 210. Of course, clock signal 220 can also originate from another source (for example, if the invention is implemented in environments other than smartcards). . . .

Within clock skipping module 240, random output 205 is used to select cycles of clock signal 220 to skip in order to produce clock signal 260. Alternatively, random output 205 can be used to select the closest corresponding cycles of clock signal 220 to be used as clock signal 260, or random output 205 can even be used as clock signal 260 itself. Still other approaches are possible . . .; the basic point being that clock signal 260 be (partially or wholly) decorrelated from external clock signal 220 via random output 205.

. . .
Additionally, clock skipping module 240 can optionally monitor the clock rate (or either clock signal 220 or 260) to prevent attackers from stopping the clock and analyzing the device in a halted state or from operating the device too quickly."

Proceeding with the Examiner's combination, the feedback shift register taught by the Moroney et al patent would most likely be driven by the single clock on line 260 produced by clock skipping module 240 or by a single clock line within the module. What this means is the clock-skipping algorithm would simultaneously affect the timing of both the linear and non-linear elements, as both

would be fed by a common clock signal. Hence, any change in the clock signal would impact the operation of both feedback elements, not just one of them.

Why, in this context, is single clock line 260 rather revealing? Because it indicates to one skilled in the art that the same clock, consisting of skipped clock pulses, as taught by the Kocher et al patent, in all likelihood would control the shift register and, as such, be applied to both the linear and non-linear feedback elements. This unequivocally means that both the linear and non-linear feedback elements would function not independently of each other but simultaneously and through that common clock signal. Consequently, both feedback elements would be active at the same time. There is simply no realistic basis for any other view as module 240 is expressly described as producing a single clock signal, not two independent clock signals.

This approach drastically differs from the present invention through which the linear and non-linear feedback elements are controlled independently of each other, which includes use of, e.g., two different clock signals: one for the linear element and another for the non-linear element, through which one element can be active while the other is not. See, e.g., paragraphs 35 and 36 on pages 6-7 of the Applicants' substitute specification, filed with their prior amendment, which describes the non-linear element as being controlled separately from the linear element such that to the former element can be deactivated while data is being loaded but the latter element remains active. Independently controlling these elements injects considerably more

complexity into their outputs, hence rendering cryptanalysis, based on, e.g., differential power analysis, considerably more difficult than if both elements, as would seem to be taught by the Kocher et al patent, were controlled through a common clock signal.

No teachings, whether express or implied, exist in the Kocher et al patent that would indicate to anyone of skill that module 240 in the arrangement in FIG. 2 should be modified to produce a second clock signal, independent of that appearing on line 260. The Kocher et al patent simply does not disclose or suggest the concept of independently controlling two separate cryptographic operations separately from each other, whether through use of two different clock signals or another technique. In fact, any such teachings would contradict the rather explicit teachings in this figure and in the text quoted above.

Moreover, no one faced with the teachings of the Kocher et al patent would even think to include to separately control the linear and non-linear feedback functions, such as through use of a second clock signal, as doing so would inject added complexity into the arrangement and seem, at least from the teachings of that patent, to be extraneous.

As such, the combined teachings of the Kocher et al and the Moroney et al patents stop far short of the present invention, as now recited in claim 15.

Independent claim 15, as it presently stands, contains suitable recitations directed at the distinguishing

features of the present invention. In particular, this claim recites as follows, with those recitations shown in a bolded typeface:

"A method for protecting a portable card, provided with a cryptographic algorithm for enciphering data and/or authenticating the card, against deriving a secret key used in the card from statistical analysis of information leaking away from the card to an outside world in the event of cryptographic operations performed by the card, the card being provided with at least a shift register having linear and non-linear feedback functions for implementing cryptographic algorithms, the method comprising the steps of:

loading data to be processed and a secret key into the shift register of the card; and

controlling the linear and non-linear feedback functions separately from each other in such a manner that collection of values of recorded leak-information signals is resistant to deriving the secret key through said statistical analysis of the values." [emphasis added]

Neither the Kocher et al or Moroney et al patents, taken singly or in any combination, including that posed by the Examiner, contains any disclosure, teachings or suggestions, whether express or implicit, of use of a shift-register based arrangement for encrypting data which includes linear and non-linear feedback elements that function separately from each other and are appropriately controlled to make detection of a secret key, through detection of leak information, increasingly resistant to statistical analysis.

As such, the Applicants submit that claim 15, as it now stands, is not rendered obvious by the teachings in the applied art, whether combined or not. Consequently, claim 15 is patentable under the provisions of 35 USC § 103.

Each of claims 16, 17 and 24 directly depends from independent claim 15 and recites further distinguishing aspects of the present invention.

Accordingly, the Applicants submit that claim 16, 17 and 24 are not rendered obvious by the teachings in the Moroney et al and Kocher et al patents for the same exact reasons set forth above regarding claim 15. As such, the Applicants submit that these dependent are patentable under the provisions of 35 USC § 103.

2. Claims 18, 19 and 23

The Examiner rejected dependent claims 18, 19 and 23, under the provisions of 35 USC § 103, as being obvious over the teachings in the Moroney et al patent in view of the Kocher et al patent, as applied to claim 15, and further in view of the Shimada patent (United States patent 6,278,780 issued to M. Shimada on August 21, 2001). This rejection is respectfully traversed.

The Examiner states that the Shimada patent discloses a method where, with respect to: (a) claim 18, after an internal key has been loaded into a shift register, the register clocks on and data bits are loaded; (b) claim 19, after the shift register has been clocked on, the contents of the shift register is filled with the initial key; and (c) claim 23, where internal keys are generated as initial keys and utilized for linear feedback shift registers, and where the contents of the shift register are fixed in that the register is always empty in order for an initial key to be loaded.

As has been discussed in the Applicants' prior amendment mailed November 4, 2005, the Shimada patent discloses a method for generating, with sufficiently high speed and security, internal keys to be set in feedback shift registers of a pseudo-random sequence generator used in a stream cipher system for use in generating pseudo-random numbers. These numbers, in turn, are combined, through an exclusive-OR operation, with a data sequence with the result either being recorded on a recording medium or transmitted in a communication system. The purpose in using this method is to prevent a third-party from tapping the data sequence without permission.

Specifically, the pseudo-random number generator, shown in FIG. 6 and described in col. 1, line 65 et seq of the Shimada patent -- which appear to be the only teachings in this patent particularly pertinent to the present invention, contains N linear or non-linear feedback shift registers S_1, \dots, S_n , each operating as a sub-generator. An internal key from keys K_1, \dots, K_n is initially applied to each corresponding one of the feedback shift registers. Each such register is then shifted by one bit and provides its least significant bit, as output, to a combination function F. Each such register generates its most significant bit from its registered bit sequence and according to a certain feedback function. The combination function F generates a key-stream bit-by-bit according to a certain combination function from outputs of feedback shift registers S_1 to S_n .

The Shimada patent, being directed simply to producing a pseudo-random sequence, is also devoid of any

teachings relevant to the problem solved by the present Applicants; namely, how to protect a smart card from external attacks arising from statistical analysis of data leakage, let alone through a feedback shift register structure that employs independently operating linear and non-linear feedback elements. All that the Shimada patent teaches is a pseudo-random number generator.

Merely incorporating such a generator as taught by the Shimada patent into a system predicated on the teachings of the Moroney et al and Kocher et al patents -- again assuming that the teachings of the latter two patents would in fact be combined by any one of skill in the art, would simply not result in a system that lies any closer to the Applicants' inventive teachings than would a system resulting from just combining the teachings in the Moroney et al and Kocher et al patents. Specifically, such a generator would simply take the place of the DFAST generator disclosed by the Moroney et al patent.

Hence, new independent claim 15 is not rendered obvious over the teachings in these three applied patents, whether taken singly or in any combination -- including that posed by the Examiner, for the same exact reasons set forth above with respect to the Moroney et al and Kocher et al patents.

Each of claims 18, 19 and 23 depends, either directly or indirectly, from independent claim 15 and recites further distinguishing aspects of the present invention. Consequently, the Applicants submit that each of these three dependent claims is not rendered obvious by the

teachings in these references. Consequently, all three of these claims are patentable over these applied references for the same reasons set forth above with respect to claim 15.

3. Claims 20, 21 and 22

The Examiner rejected dependent claims 20-22, under the provisions of 35 USC § 103, as being obvious over the teachings in the Moroney et al patent in view of the Kocher et al patent, as applied to claim 15, and further in view of the Rose patent (United States patent 6,510,228 issued to G. G. Rose on January 21, 2003). This rejection is also respectfully traversed.

The Examiner states that the Rose patent discloses a method where, with respect to: (a) claim 21, during a clocking interval, an output is not generated and hence no new data is loaded into a shift register during or prior to that clocking; and (b) claims 20 and 22, since the input data is not being loaded into the shift register, the data is not connected to that register during that interval.

Specifically and also as discussed in the Applicants' prior amendment mailed November 4, 2005, the Rose patent discloses a method and apparatus for generating encryption stream ciphers, and in particular an encryption bit stream for use therein. Here, the bit stream is generated through use of a recurrence relation designed to operate over finite fields larger than a Galois Field of order 2.

A linear feedback register, which can be realized using a circular buffer or sliding window, implements the recurrence relation. See, e.g., col. 2, line 26 et seq of this patent. As noted in col. 3, line 1 et seq, linearity is removed from the output of the shift register through use of one or a combination of various processes: irregular stuttering (also referred to as decimation), a non-linear function, multiple shift registers coupled with combining the outputs of the registers, a variable feedback polynomial on one register, and other non-linear processes. Further and as indicated in col. 3, line 10 et seq, a non-linear output can be derived by performing a non-linear operation on selected elements of the shift register.

For example, in the exemplary embodiment shown in FIG. 4 and as discussed in col. 10, lines 54 et seq of the Rose patent, stuttering and a non-linear function are used to remove the linearity of 16-byte shift register 52 from its output. The non-linear function is multiplication (62) of sums formed by modulo 256 adders 60a and 60b to which the values of four specific bytes in the register (S_n and S_{n+5} ; and S_{n+2} and S_{n+12} , respectively) are collectively applied. Since the non-linear output derived from the state of the linear feedback shift register may (still) be used to reconstruct the state of the shift register, stuttering is introduced to render this reconstruction more difficult. Stuttering is performed by not representing some of the states at the output of the generator, and choosing which do so appear but in an unpredictable manner. To implement this, the non-linear output determines what subsequent bytes of the non-linear output appear in the output encryption bit stream. This is accomplished by

Appl. No. 10/019,344
Amdt. dated June 26, 2006
Reply to final Office action of Jan. 26, 2006

switch 68, buffer 70, multiplexer 64 and exclusive OR gate 66. See, col. 11, line 60 through col. 12, line 63.

The Rose patent, being directed to a encryption bit stream generator for use in a stream cipher, is also devoid, just like the Shimada patent is, of any teachings relevant to the problem solved by the present Applicants; namely, how to protect a smart card from external attacks arising from statistical analysis of data leakage, let alone through use of a feedback shift register structure that employs independently operating linear and non-linear feedback elements.

Merely incorporating an encryption bit stream generator as taught by the Rose patent into a system predicated on the teachings of the Moroney et al and Kocher et al patents -- here too assuming that the teachings of the latter two patents would in fact be combined by any one of skill in the art, would simply not result in a system that lies any closer to the Applicants' inventive teachings than would a system resulting from just combining the teachings in the Moroney et al and Kocher et al patents. Specifically, such a bit stream generator, though suitably modified for use in a block cipher, could simply be another way to generate a keystream and thus could be substituted for the DFAST generator disclosed by the Moroney et al patent.

Hence, new independent claim 15 is not rendered obvious over the teachings in these three applied patents, whether taken singly or in any combination -- including that posed by the Examiner, for the same exact reasons set forth

Appl. No. 10/019,344
Amdt. dated June 26, 2006
Reply to final Office action of Jan. 26, 2006

above with respect to the Moroney et al and Kocher et al patents.

Each of claims 20-22 depends, either directly or indirectly, from independent claim 15 and recites further distinguishing aspects of the present invention. Consequently, the Applicants submit that each of these two dependent claims is not rendered obvious by the teachings in these references. Hence, each of these three claims is patentable over the Moroney et al, Kocher et al and Rose patents for the same reasons set forth above with respect to claim 15.

Conclusion

Consequently, the Applicants submit that none of the claims, presently in the application, is obvious under the provisions of 35 USC § 103. Thus, the Applicants believe that all their present claims are in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

Respectfully submitted,


Peter L. Michaelson
Peter L. Michaelson, Attorney
Reg. No. 30,090
Customer No. 007265
(732) 542-7800

June 26, 2006

MICHAELSON & ASSOCIATES
Counselors at Law
P.O. Box 8489
Red Bank, New Jersey 07701-8489